



THE SMALL BOOK OF TERMS ~~AND~~ INSTRUCTION

WELCOME TO CYBER FOR SCHOOLS

This small cyber book will introduce you a wide range of security terms, commands and tools that will be needed for a successful game session!

And this is not even the coolest part!

Equivalents of **attack** and **defence** in security are the red team and blue team respectively.

You will learn your duties, responsibilities and knowledge needed to dive on each of the game's episodes.

The reds will use the Linux as their Virtual Machine of choice to solve their tasks, which will mainly include simulation of hacker's malicious activities. The blues on the other hand will be using Windows and will have to stay vigilant to detect and recognize malicious activity, links or attachments.

Notes: This book's purpose is to introduce pupils to the knowledge needed to perform the Cyber4School game's episodes.

What we recommend: The pupils and teachers should use this book BEFORE they play the game. This can be done in forms of lessons/training, to make sure the NEW concepts are properly grasped by the pupils.

We understand that cybersecurity might be a new term for the younger generation. For this reason, only after all participants are familiarized with the (new) content, the game should be played.

EPISODE 1: PHISHING

In this episode, Blues and Reds will be introduced to Phishing. You might have probably heard of this term before!

Hackers use multiple ways to trick people to give away their personal information, and later hack them. This family of techniques that uses psychological manipulation to trick people into giving away secret or confidential information is called *social engineering*.

The most famous social engineering technique is *Phishing*, in which hackers send (often very normal looking) malicious messages or e-mails to the victims. Through these e-mails they ask the receiver to give away private information, push/urge them to click on malicious links (websites), or even attach malicious files that could cause trouble if downloaded/opened by the receiver.

In this episode, something like this might happen, so you need to stay vigilant.

How does a phishing e-mail look like:

- Language: Sometimes it requires immediate action from you!
- Grammar: Look out for grammatical mistakes. Sometimes they have plenty!
- Pictures, Logos and Footers: All these might make you think the e-mail is coming from a legitimate person. Do not be fooled!
- Attachments: You should know that the delivery of the malicious files is through this e-mail, so it is highly possible that the file contains a malware!
- Links: Links included on the e-mail could be quite dangerous. Are they safe? Be careful not to click them without making sure...

Some preventive measures you should keep in mind:

- Think: Was this e-mail expected? Why is it this urgent?
- For attachments: Do not download anything without making sure what it is!
- For links: Use mouse hovering! Check the e-mail source code to learn more about the e-mail.

But what is mouse hovering? How can I tell a website is safe at a first glance? What is the e-mail source code?

Mouse Hovering is a simple technique you can do with your mouse by moving it to the link attached. If you are lucky enough, you will see the real website's name.

HTTP and HTTPS are the very first letters we see when we are browsing on the internet on the very top box. These two are both protocols used on the internet in order to transfer data. When a website is using HTTP, it is not secure! This means everything we type on the website such as username, passwords, e-mails, etc. can be easily captured by a malicious person.

HTTPS on the other hand is secure! Remember the **S** stands for SECURE! This means everything we type on a website will be difficult to understand for a malicious actor, as it will be *encrypted*, or changed from its original form when is being transferred.

The anatomy of a website:



- | | |
|-------------|--------------------------|
| 1 Protocol | 4 Top-Level Domain (TLD) |
| 2 Subdomain | 5 Subfolder |
| 3 Domain | 6 Slug |

E-mail source code investigation or just investigating the **header of an e-mail**, sometimes can help us to determine the legitimacy of an e-mail. Below is an example of an e-mail source code, which format is quite different from what we have seen. However, we can get a lot of information from it! Let's see what is important! You teacher will guide you how to go there from the mail service you are using!

```
Received: from [SOME IP] (port=17671 helo=mta-out.someip.example)
  by mail.someone.com esmtps (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  (Exim 4.94.2)
  (envelope-from <hacker27@somedomain.com>)
  id 1nzdVh-00005X-RV
  for digiblu@mailfence.com; Fri, 10 Jun 2022 14:13:05 +0200
Received: from mail.somedomain.com
  Microsoft SMTP Server (version=TLS1_2,
  cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.986.22; Fri, 10 Jun
  2022 14:14:25 +0200
Received: from [192.168.27.2] (unknown [192.0.27.1])
  by smtp.someIP.example
  15.02.0986.022; Fri, 10 Jun 2022 14:14:25 +0200
From: American B. <hacker27@somedomain.com>
To: "digiblu@mailfence.com" <digiblu@mailfence.com>
Subject: YOU HAVE BEEN SELECTED AS A WINNER!
Thread-Topic: YOU HAVE BEEN SELECTED AS WINNER!
Thread-Index: Adh8wvf0KMBZi3i0T9SnG7PO/oCtyw==
Date: Fri, 10 Jun 2022 12:14:25 +0000
Message-ID: <45929aca81c648bca4ae44f18b14bebc@uniss.org>
Accept-Language: en-GB, de-DE, en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-originating-ip: [Some_IP_Here]
Content-Type: multipart/mixed;
  boundary="_004_45929aca81c648bca4ae44f18b14bebcunissorg_"
MIME-Version: 1.0
X-Spam-Flag: NO
X-Spam-Status: No, hits=1.2 required=4.7 symbols=HTML_MESSAGE,SPF_HELO_NONE,SPF_SOFTFAIL,SUBJ_ALL_CAPS,T_HK_SPAMMY_FILENAME,T_SCC
Delivered-To: digiblu@mailfence.com
```

You see, there are three **Received chains**. Think of these as the places or servers the e-mail has hopped in order to get to you.

The last **Received** is more important as it shows the internet protocol or *IP* of the sender.

Other information you can get: the exact time and date, the real e-mail address of the sender, the subject, the real domain where the e-mail is coming from, etc. can all be identified. Ignore the rest of information if not needed or if it's too complicated.

Did you know:

- Microsoft is the most impersonated brand globally when it comes to phishing attempts! People fall for it!
- The most common data types that are stolen from phishing e-mails are: Credentials (usernames and passwords), personal data (phone numbers and e-mail addresses), medical data and banking data (credit card information).
- Brazil is the country with the highest number of phishing e-mails at the moment!

INFORMATION FOR THE BLUES:

- You should stay vigilant and pay attention to all the up-mentioned information
- You will be using Windows to solve this first episode as well as the others
- You will be provided extra tools on Windows in order to check out the malicious link; check them out and paste the link there without clicking

INFORMATION FOR THE REDS:

- In order to create a phishing e-mail, you should also take notice of the above
- You should try hard to mimic a real person or appear legitimate!
- You will be using Linux terminal, which is a place to help you easy operate into the system, or do whatever activity you want just by writing some easy commands
- In order to ease the creation of a malicious website which will be placed on your phishing e-mail, below you can find a table of commands to use in terminal (to have your own fun time!) or Aliases (or simple commands we created for you) to make the process easier
- The commands below can be used for any of the episodes, while aliases are unique for each of the episodes!

Aliases, commands and tools for Reds

Check “Tools and their Details” folder inside the Episode1 folder on Desktop, to learn more about the adjusted tools you will use.

When you are asked to provide the password in order to run commands, type: kali

create_bad_link – This will redirect you to a “portal” where you can create your own malicious link, where you have to follow steps on the screen based on your preferences

where_is_data – This command will send allow you to see in which file the data is saved and how it is named. Note: This command views the filename but the content you have to check yourself!

prepare_bad_email – This will redirect you to a portal where you can step-by-step prepare a phishing e-mail, which you will test yourself.

whoami – Ask the terminal this and you will get your username

cd – It stands for “Change Directory” and with this command you can switch from one folder to another. Type cd followed by the path of the directory you want to go. Example: to go to episode 1 folder, **cd Desktop/Episode1/FolderName/FolderName**

python3 – This command followed by the name of the python script (file) will execute the file. Example **python3 scriptName.py**

ls – This command will list you all the files inside one directory or folder

mkdir – This command is used to create a new directory or folder

mv – This command is used for moving and renaming files or folders inside a directory

pwd – This stands for “Print Current Directory” and you will get the location or the folder you are in; you can be in Desktop, or inside any folder

nano – Nano is a text editor tool you can use to view the content of a file from the terminal

date – It displays the system’s date and time

cp – A command to copy files

sudo – Using this before every command, will let you execute anything as an administrator! Be ready to type the VM-s password a lot...

Running a script (step by step):

1. Open the terminal by searching for it in the dashboard or pressing Ctrl + Alt + T .
2. Navigate the terminal to the directory where the script is located using the cd command.
3. Type **python3 scriptname.py** in the terminal to execute the script.

EPISODE 2: MALWARE (Spear phishing)

In addition to the malicious links, there are also malicious attachments that if downloaded, can harm our computer. These malicious software are called **malware**. Depending on their type, they can affect our computer in different ways, such as infect it, steal the data inside, encrypt the data (or make them inaccessible/unreadable), or conduct any other behaviour that the attacker wants.

RANSOMWARE:

In this episode, you will have a closer look at the malware called **Ransomware**. The behaviour of the ransomware looks like this: After installed on the computer, it will search for specific files and make them inaccessible from you (or else *encrypt* them), until you pay a certain amount of money (or *ransom*) that the attacker has demanded from you. Usually, there is always a message on your screen informing you that your files have been encrypted, and you need to pay money to get the key from the attacker in order to decrypt them, or else get them back. This is called a *ransom note*. Your files are held for ransom (the amount to be paid), and that's where the name of the malware is derived from.

But first, let's talk a bit about encryption. Encryption allows the data to be hidden or not readable from humans, and it is done with a secret code or a key. When the ransomware locks our files, the files are said to be *encrypted*. The opposite process is called decryption, and it is the process of changing the encrypted information back to *plaintext*, or else readable text, with the use of a secret key. This key can be the same as the encryption key (called symmetric encryption), or different from it (called asymmetric encryption). Below is a schema of "Hello" message that is first in plaintext, encrypted in the second block so you can only see symbols, and decrypted in the third block where you can again read it!

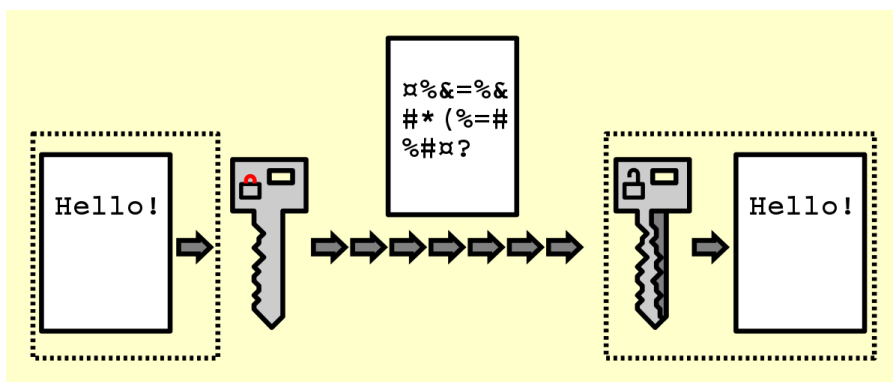


Figure 1:
Encryption/Decryption,
Source:
<https://en.wikipedia.org/wiki/Encryption>









How does a ransomware note look like after files get encrypted? On the left is an example of it!

Figure 2: Nitro Ransomware note,
Source:
<https://i0.wp.com/howtofix.guide/wp-content/uploads/2021/04/giveme-nitro-ransom-note.jpg?resize=810%2C560&ssl=1>

OTHER MALWARE:

Below is a table of the types of most common dangerous malwares that exists:

 <p>Ransomware: Malware designed to block the access to a system (through the encryption of the data) until a certain amount of money is paid.</p> <p>Examples: NotPetya, SamSam, Maze, WannaCry, Locky, GrandCrab, etc.</p>	 <p>Trojans: Maliciously designed malware that gets access to a system by appearing as harmless.</p> <p>Fun Fact: The name is derived from the infamous Trojan Horse from Ancient Greece that led to the fall of Troy.</p>
 <p>Worms: A standalone malware that replicates itself in order to spread to other computers by using different means.</p> <p>Fun Fact: The first computer worm was devised to be an Anti-Virus software.</p>	 <p>Logic Bomb: A malicious piece of code inserted into a software which sets off harmful actions if certain conditions are met.</p> <p>Fun Fact: Viruses and Worms may contain Logic Bombs in order to spread unnoticed.</p>
 <p>Spyware: Malware designed to gather your personal computer data and forward it to a third-party without consent.</p> <p>Fun Fact: Data compromised include Login Credentials, PINs, Credit Card details, Browsing Habits, etc.</p>	 <p>Backdoor: A means to access the computer system or encrypted data that bypasses the security mechanisms.</p> <p>Fun Fact: The infamous SolarWinds attack was assisted by a backdoor installed on the code of the company's software. It remained undetected for a long time.</p>

OBFUSCATION:

Obfuscation is a technique commonly used by hackers in order to create or alter data to make it difficult to read or interpret. This way, they will hide the behaviour patterns of the malware as well as bypass the detection (usually by the AntiVirus).

BASE64:

While there are many obfuscation techniques, you will hand on practice the **base64 encoding**. This simple malware obfuscation technique converts or alters the desired scripts into strings, only using 64 characters. This is where the name is derived as well. The opposite action is called **decoding**.

These characters include A-Z, a-z, 0-9, +, /, =.

[Full list: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=]

Encoding and encryption, from a broader view, seem to do the same thing. However, there are major differences between the two. These are shown in the table below:

<p>Encryption Transforms, or alters data into another format to keep it a secret from others. This secret (encrypted data) can only be reversed or decrypted possessing specific knowledge, such as the key for decryption. Only specific people could perform this.</p> <p>It is used to maintain data confidentiality.</p>	<p>Encoding Transforming or altering the data into another format, so it can be transmitted safely, without any danger of being manipulated. It uses a scheme that is publicly available, so decoding the encoded data is easily done.</p> <p>It is used for maintaining data usability.</p>
---	---

Did you know:

- The first ever ransomware is called AIDS Trojan or PC Cyborg Trojan created by a biology professor called Joseph Popp.
- Phishing is one of the most common ways for the Ransomware to reach your computer.
- 95% of the Ransomware files are executables suitable to run only on Windows.

INFORMATION FOR THE BLUES:

- You will also be provided a decryptor at your hands.
- Be careful! You should first examine it and eventually perform decoding.
- Will you be able to get your files back?

INFORMATION FOR THE REDS:

- You will still behave like the bad guys and play with a malware script!
- You will be able to edit and customize it as you wish and test it on your system.
- You will perform encoding to ensure you remain undetectable.

<p>Useful commands and tools for Blues</p> <p>Cmd – Command line interface for Windows, where you can run multiple commands or else interact with your computer directly using these commands. Refer to the folders inside the episode on how to use and access it.</p> <p>Notepad++ - Text editor tool to assist you in viewing text files.</p> <p>DROID – A tool for the filetype identification. Refer to the folders inside the episode on how to use it.</p> <p>Certutil base64– A cmd command to perform encoding and decoding.</p> <p>Example of its use: certutil -encode my_data.txt encoded_data.txt</p> <p>Example explained: certutil (name of the tool initiated) -encode (action to perform) my_data.txt (file where data I want to encode is saved) encoded_data.txt (new file where data inside is encoded)</p> <p>Base64decode.org – Online tool to assist you with the decoding of the encoded file/text.</p> <p>Base64encode.org - Online tool to assist you with the encoding of the decoded file/text.</p>
--

Aliases, commands, and tools for Reds

When you are asked to provide the password in order to run commands, type: kali

edit_script = You can freely edit parts of the script that will encrypt the files

run_malware = Will run the malware and then you will see its consequences.

run_decryptor= Will run the decryption script, so you can possibly read your files again.

base64 – A terminal command to perform encoding and decoding.

Example of its use: `base64 simple_text.txt -w 0 > encoded.txt`

Example explained: `base64` (name of command initiated) `simple_text.txt` (the file I want to encode) `-w 0` (this option will save the outputted encoded text into one line only, so wrapping is 0) `>` (arrow indicating that the output will be saved somewhere with a specific name) `encoded.txt` (this is the name of the file I chose for the encoded output that will come from the execution of the command)

Base64decode.org – Online tool to assist you with the decoding of the encoded file/text.

Base64encode.org - Online tool to assist you with the encoding of the decoded file/text.

Running a script (step by step):

1. Open the *terminal* by searching for it in the dashboard or pressing Ctrl + Alt + T
2. Navigate the terminal to the directory where the script is located using the cd command
3. Type `python3 scriptname.py` in the terminal to execute the script.

EPISODE 3: NETWORK SECURITY

NETWORK AND INTERNET

A network is simply a group of computers which can communicate to each-other by using common protocols (or rules). They may be interconnected through different telecommunication network technologies, such as wired, wireless, etc. and they may also share resources, such as internet, applications, or printers.

While a network is a group of two or more computers, internet on the other hand is the interrelationship of a few networks and connects millions of people all over the world. It is also called the “network of networks”.

WI-FI: SECURE VS INSECURE

Wi-Fi stands for Wireless Fidelity, and it is a networking technology that uses radio waves for data transmission over short distances. Is it very often used to link computers in small geographical areas, called LAN (Local Area Networks), and it operates without cables or wiring!

Wi-fi is used widely to provide Internet access for various wireless-enabled devices, such as laptops, smartphones, etc. The areas that provide Wi-fi access, else called “hot spots” or “access points”, have become very common and can be found almost everywhere: airports, cafes, restaurants, bookstores, etc.

There are secured and unsecured Wi-Fi networks.

- Spotting the unsecured ones: They do not have a security encryption key and everybody can connect and begin browsing. *They do not usually require a password.*
- Spotting the secured ones: The secured networks are usually locked with a security encryption key. *In simpler terms, they require a password.*

HONEY-POTS

Hackers sometimes create their own “legitimate looking” access points by duplicating the real legitimate ones. They do so in order to trap the users into connecting to them. Very often they succeed in trapping them, as many of us would connect to a free Wi-fi!

The moment the users are connected, the hackers can see, intercept and even modify the network traffic (the data being moved across). So someone might receive something different from what I actually sent!

All links should be treated with suspicion while browsing on unsecured networks.

For example, accessing the websites without the *HTTPS*, would compromise the device encryption and allow other malicious users on the network to view the information being sent to the device.

HTTPS adds a security layer so that even in case of interception, the communication is encrypted and cannot be read.

Fun-fact: Man-in-the-Middle

MITM (man-in-the-middle) is an attack where a malicious person stands secretly between two parties and can intercept and possibly alter (change) the communication between the two. The attacker is not only able to intercept all the messages passed in between the victims but also inject new ones.

APACHE WEB SERVER IN LINUX

Apache is one of the most used Web Servers in Linux. Web servers are used to view and serve different Websites or Web pages that are requested from the client computers. Having Apache server installed, allows us to host (“publish”) our own website.

The location where the website files and folder are usually located in Linux is “*/var/www/html*”. You should have the “rights” to operate within these folders.

INFORMATION FOR THE **BLUES**:

- You will be able to connect to available Wi-Fis
- You will be able to notice the difference between the secured and unsecured access points
- As you connect to different access points, you will access different websites and notice what is special about them

INFORMATION FOR THE **REDS**:

- You will clone a legitimate website using tools that previous attackers have created and host it on your Apache server
- You will be able to notice the key differences between the two websites
- You will try to manipulate the network, in order to be able to see and access the latest files uploaded on the cloned website

Useful commands and tools for Blues

Cmd – Command line interface for Windows, where you can run multiple commands or else interact with your computer directly using these commands. Refer to the folders inside the episode on how to use and access it.

Notepad++ - Text editor tool to assist you in viewing text files.

Aliases, commands, and tools for Reds

When you are asked to provide the password in order to run commands, type: kali
Website files in Linux are placed here so you can manually check them: /var/www/html

Aliases:

open_original_website – This helpful command will open the original Digischool's website

view_uploaded_file – After the project upload attempt, this command will confirm whether you can see the file or not. If you are able to view the file, it means you do not have access to view the uploads

copy_website – This command will help you to create a copy of the original Digischool's website

start_server – This command will start your own web application server, which will allow you to run your own Digischool's website copy!

get_rights – This command will give you some rights to perform certain actions as an administrator

open_fake_website – This command will open the fake copied website you created earlier on the browser!

View_upload – This command opens the latest uploaded file on the **copied** digischool's website. If you can view it, the process was a success!

Useful commands:

cd – It stands for "Change Directory" and with this command you can switch from one folder to another.

Ls – This command will list you all the files inside one directory or folder

mkdir – This command is used to create a new directory or folder

mv – This command is used for moving and renaming files or folders inside a directory

pwd – This stands for "Print Current Directory" and you will get the location or the folder you are in; you can be in Desktop, or inside any folder

nano – Nano is a text editor tool you can use to view the content of a file from the terminal

cp – A command to copy files

sudo – Using this before every command, will let you execute anything as an administrator! Be ready to type the VM-s password a lot...

EPISODE 4: PASSWORD SECURITY

PASSWORDS

Passwords are like secret codes that are used to protect something important online. Perhaps, an e-mail account or a cell phone PIN. Passwords are important means for providing security and protection of sensitive information from unauthorized access, potential threats, thieves, or hackers! They are also a form of “authentication”, as they are used to verify the identity of a user trying to get access (example: someone tries to log in on Facebook).

For this reason and more, keep them safe and do not share!

STRONG PASSWORDS

It is very common for our passwords to be guessed (cracked, stolen or brute forced) from others! To prevent unauthorized access to your accounts and sensitive data, it is important to create a strong password. A strong password takes a looonooog time to guess (theoretically: even years, or decades!), thus it brings you a more maintained security and privacy in the digital age.

How does a strong password look like? Below are some main characteristics of strong passwords, recommended for everyone to follow.

- Lengthwise: The longer, the better! If you could remember a 12–14-character long password, that would be great!
- Complexity: They should contain a mix of numbers, symbols, upper and lowercase letters.
- Uniqueness: Strong passwords are not reused across multiple accounts! Don’t give the hacker the pleasure to steal all your accounts, just because they managed to steal 1 password!
- Randomness: Strong passwords should not necessarily be something that hold a meaning (a word or a phrase), as sometimes they can also be guessed! Also: no birthdates, addresses or names! Keep it as random as you can!

A *strong password* would look like: [@{Yb3rf0r\\$\(h00L\\$202E](#).

Now it’s your turn to create one: _____

COMMON PASSWORDS

Some common passwords that are frequently used include very simple memorable words or phrases, such as: “password”, “qwerty”, “letmein”, “iloveyou”, “admin”, or “football”.

These passwords are very short in length, easy to guess and even to crack with brute force or dictionary (will explain these methods further below). In fact, the time to crack these passwords through these methods is “instant”. The below table will explain this...

Through the below table you can also calculate how strong your password is and how fast it can be cracked.

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets, symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Figure 3: How long it takes to crack a password, source: CloudNine.com

GUESSING PASSWORDS

Sadly, passwords are often guessed from unauthorized people. The weaker the password, the easier it is to guess. However, there are several ways that somebody could steal or crack your password that you should be mindful about:

- Through *social engineering*: This method tricks you into giving your password away, usually by impersonating a trusted source that is requesting the password.
- *Phishing*: Usually there are fake login pages created by malicious users (that look exactly like the real ones!), that trick the user into typing their password which is then captured and stolen.
- *Brute force attack*: This is a very known method of password cracking in which every possible combination of characters is tried out until the correct password is guessed. This is done usually through the use of software and specific password-cracking tools (such as Hydra in Linux).
- *Dictionary attack*: Instead of single characters combination, this method tries out a list of common words, phrases, or commonly used passwords to guess the correct one. These attempts are also usually performed by software and tools.

SHOULDER SURFING

Have you ever been in a very crowded public place and typed sensitive information on your phone or laptop? There is a security threat related to situations like this, and it is called shoulder surfing. In this type of threat, the malicious person is standing close to you, close to your *shoulder*, or in front of your screen's reflection while you type passwords and other sensitive data on your devices.

Shoulder surfing can also be performed through cameras or binoculars! For this reason, it is very important to be aware of your surroundings and take steps to shield your information.

PASSWORD-CRACKING TOOL: HYDRA (HOW TO USE IT)

As briefly mentioned before, password cracking is the attempt to guess or retrieve a password in various ways, including brute force or dictionary attacks, or even manual combinations until the correct password is found. There are numerous password cracking tools available to use in Windows and Linux, including: hashcat, hydra, medusa, or john the ripper.

In this episode, Hydra is used as the password-cracking tool of choice. A simple explanation of the tool is made below. To learn more about Hydra and how to use it, type `hydra -h` on terminal (linux)!

```

kali@kali: ~
└─$ sudo hydra -l digiblu@project.net -t 2 -P /home/kali/Desktop/Episode4/Red/wordlist.txt 127.0.0.1 http-post-form "/digiblu_secret_page/index.php?user='USER'&password='PASS':Invalid user or password."
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-13 18:58:36
[DATA] max 2 tasks per 1 server, overall 2 tasks, 101 login tries (11:pi101), "51 tries per task
[DATA] attacking http-post-form://127.0.0.1:80/digiblu_secret_page/index.php?user='USER'&password='PASS':Invalid user or password.
[90][http-post-form] host: 127.0.0.1 login: digiblu@project.net password: ██████████
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-13 18:58:39

```

Figure 4: How to use Hydra, Linux Terminal

sudo →	run a command as another user (admin)
hydra →	the name of the password cracking tool
-l →	a parameter for which you must specify the login name (or e-mail, or file with login names); In this case <code>digiblu@project.net</code> is the e-mail to login
-t →	number of tasks (attempts) specifies; in this case is 2
-P →	a parameter for which you must specify the password, or the file which contains a list of passwords to try for the brute force; in this case, the <code>wordlist.txt</code> file is used (and its location is also specified)
the rest	further on the command, the target is specified (127.0.0.1), as well as the login form where <code>USER</code> and <code>PASSWORD</code> should match the correct one

The results in green confirm that the user “`digiblu@project.net`” has a password which was successfully found! (it is covered with a blue sticker for security reasons...)

Useful commands and tools for Blues

Cmd – Command line interface for Windows, where you can run multiple commands or else interact with your computer directly using these commands. Refer to the folders inside the episode on how to use and access it.

Notepad++ - Text editor tool to assist you in viewing text files.

Aliases, commands, and tools for Reds

When you are asked to provide the password in order to run commands, type: kali

whoami – Ask the terminal this and you will get your username

cd – It stands for “Change Directory” and with this command you can switch from one folder to another.

ls – This command will list you all the files inside one directory or folder

mkdir – This command is used to create a new directory or folder

mv – This command is used for moving and renaming files or folders inside a directory

pwd – This stands for “Print Current Directory” and you will get the location or the folder you are in; you can be in Desktop, or inside any folder

nano – Nano is a text editor tool you can use to view the content of a file from the terminal

date – It displays the system’s date and time

cp – A command to copy files

sudo – Using this before every command, will let you execute anything as an administrator! Be ready to type the VM-s password a lot...

INFORMATION FOR THE BLUES:

- You will be able to examine a camera login page and perform a type of shoulder surfing, seeing what it has captured
- You will have the opportunity to test your own website's security, by trying to manually "brute force" or guess the login password

INFORMATION FOR THE REDS:

- You will perform a type of shoulder surfing by examining what a camera has captured
- You will land on the DigiBlue Login page, a page you should not normally find!
- You will try to automatically brute force and guess the login password for this page
- If successful, you will find out about the secret project the Blue team is hiding!

EPISODE 5: WEBSITE SECURITY

You can visit different *places* while surfing on the internet, as many *websites* are available and they allow you to play games, shop, learn new things or just have fun! These websites are built for different purposes and are created by web developers who use different codes to make them work well, look good and also be secured from different website attacks.

A website needs to be secured for different reasons, such as:

- to maintain availability to the visitors (some attacks can make websites shut down completely or slow down);
- to protect the user's data (some website attacks allow bad actors to steal user's personal data);
- to maintain the website's integrity (some attacks include injection of malicious code that can modify, delete or steal its content);
- etc.

OWASP AND "OWASP TOP 10"

OWASP stands for Open Web Application Security Project, and it is a group of people dedicated to make internet a safer place for everybody. OWASP, every few years prepares and updates a list of the most common website vulnerabilities. This is called the "OWASP Top 10" and helps people all around the world to stay aware of the most significant web threats.

OWASP WEBSITE VULNERABILITIES

Below there are some of the most significant website vulnerabilities taken from the "OWASP top 10", which we have tried to explain in a simple way. One of these vulnerabilities will be present on the Episode's 5 website, so try to understand what each of them means and how to detect it...

- 1) *Broken Access Control*: In Order to access a website, you mostly have to enter your username and your password. That process is called authentication. During that process your authorization level will be determined it will grant you access to specific content and functions. A breach for example happens if someone falsely accepts your request to more actions that should not have been granted to you.
- 2) *Insecure design*: Sometimes, even if you design software well, there can be hidden mistakes in how it was designed or built that could be dangerous. These mistakes can happen if the people making it didn't think enough about how to keep it safe. To make sure something is safe, the people making it need to always be thinking about what could go wrong and test it to make sure it can't be hurt by hackers.
- 3) *Security misconfigurations*: Security misconfiguration occurs when security settings are not adequately defined in the configuration process or maintained and deployed with default settings. For example, you get a new PC. During the setup you don't change your password and keep the default password 'admin'. While you leave your room someone else enters who also got the same PC as you and therefore knows the default password. This person has now the ability to access your PC without your knowledge.
- 4) *Vulnerable and outdated components*: Nowadays a huge Team of managers and developers work on the development of code. Not every developer knows exactly what the other developer wrote and the visibility into what's running is very low. When components are not updated regularly, or specific component updates aren't compatible with the other components vulnerabilities will arise. But it's a hard job to keep an overlook of all components, their dependencies and remove those, that aren't necessary anymore.
- 5) *Injections*: Injections in cybersecurity are a way for hackers to put malicious code or data into a computer system. This can happen when the website or application doesn't properly validate user input, allowing the attacker to enter code or data that can then be executed by the website or application. This malicious code can steal important information, like passwords or bank account numbers, or they can make the computer not work properly, or even modify content. That's why it's important to have strong security measures in place.

INJECTION COMMANDS: ECHO

Although there are many different methods of injection, utilizing numerous commands, we will focus on a simple, yet very powerful command called *echo*. This command will also be used on Episode 5, in order to "exploit" the website which is vulnerable to injection!

The echo() command is used to display a string provided by the user. It can include different variables, filenames, and directories. It is also used to *inject code* into a web application's query string (or any box that requires user's input), tricking the application into executing commands. This can lead to unauthorized access to sensitive data, and even modification of existing website content...

The last statement is the perfect case for red team who craves to get the highest points in the table of results and win the first prize of the Science Fair event.

Try the echo command yourself! Below options also can help you to utilize your commands.

[Check this website for more: <https://phoenixnap.com/kb/echo-command-linux>]

- n: Displays the output while omitting the newline after it.
- E: The default option, disables the interpretation of escape characters.
- e: Enables the interpretation of the following escape characters:
 - \\: Displays a backslash character (\).
 - \a: Plays a sound alert when displaying the output.
 - \b: Creates a backspace character, equivalent to pressing **Backspace**.
 - \c: Omits any output following the escape character.
 - \e: The escape character, equivalent to pressing **Esc**.
 - \f: The form feed character, causes the printer to automatically advance to the start of the next page.
 - \n: Adds a new line to the output.
 - \r: Performs a carriage return.
 - \t: Creates horizontal tab spaces.
 - \v: Creates vertical tab spaces.

Other examples to try out:

- Try this command on Linux and check the output:
echo -e 'Hello, \nWorld! \nThis \nls \nCyber4Schools!'
- How to echo text into a file (could also be a hidden file inside the website!)
echo someee text > file.txt
- The following command will be used on this episode and will replace the table of results (a simple file) with the given points. Try it out on your own and master it! (Also be careful and find out in which box exactly this code should be run!)
echo "27\n40\n80\n60\n27 > results"

HIDDEN WEB SERVER FILES: WHAT ARE THEY AND WHERE TO FIND THEM

Web server hidden files are files that normally should not be visible or accessible by the visitors of the website, but they are still present on the web server! They usually contain sensitive information that helps the web server perform certain actions.

As mentioned, these files cannot be easily visible to the website visitor, but there are different ways that visitors can check for these files! On this episode, we will be using a tool called "*dirb*", which is a website content scanner that looks for existing and hidden files. It works by launching a dictionary-based attack (that means there is a file with a list of words to be tested!) against a web server and analysing the responses. If successful, you will receive a list of new URL-s for you to manually check on your web browser!

dir1 Tool syntax (kali Linux) is as follows:

```
dirb http://192.168.x.x/ /usr/share/wordlists/dirb/common.txt
dirb http://nameOfWebsite.com /usr/share/wordlists/dirb/common.txt
```

dirb →	The name of the tool
http://192.168.x.x/ or http://nameOfWebsite.com →	The name of the URL (website) to be checked for hidden directories/files
/usr/share/wordlists/dirb/ →	The location where the file containing the words to be tested is located
common.txt →	This is the name of the file that contains the possible words that might match the names of the hidden directories or files of the specified website/URL

URL ENCODING/DECODING

URL encoding is a technique used to convert special characters and spaces in a URL into a suitable format that can be transmitted over the internet. This conversion involves replacing special characters with their respective *percent-encoded values*. For example, (blank) space is replaced with "%20" or with the plus sign (+), or question mark (?) is replaced with "%3F".

Conversely, URL decoding involves the conversion of percent-encoded characters in a URL back to their original forms. This process is essential since certain characters have specific meanings in URLs, like the forward slash "/" that serves to separate different sections of a URL.

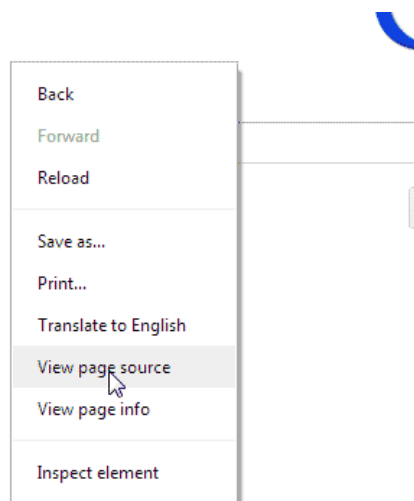
More examples of special characters and their respective percent-encoded values are shown below:

+ is equal to space
%22 is equal to "
%5C is equal to \
%3E is equal to >

WEBSITE/PAGE SOURCE CODE: WHAT IS IT AND HOW TO FIND IT

A website source code can be defined as the underlying part of a website, which contains written code from developers. They are usually written in HTML, CSS and JavaScript. Changing the source code will allow developers to modify the website content or functionality.

Checking for the website source code is made easy through right clicking on the website's background and selecting "View Source Code". As you right-click, you should normally receive a box like the below screenshot:



Viewing the website source code can sometimes be really helpful for those looking to attack or gather information on how to exploit a website. Hackers can directly look for vulnerabilities inside this code, or else gather hints and see information they should not normally see...

IOC (INDICATORS OF COMPROMISE)

Indicators of Compromise or IOC, are digital "clues" that help information security professionals to identify malicious activity or security threats. This includes data breaches, insider threats or malware attacks.

Note that this "piece of forensics data" is usually found in system log entries or files! Keep this in mind for this episode, as you will be checking for them!

INFORMATION FOR THE BLUES:

- You will be able to examine the Digischool's website and find out whether something rather suspicious has happened to the "Competition's result" page
- You will test this website for known vulnerabilities and find out if it "suffers" from any
- You will use indicators and hints given on the website: they will guide and help you!
- After identifying the Digischool's vulnerability, the Blues will try to fix it!

INFORMATION FOR THE REDS:

- You will be able to examine Digischool's website and "hunt" for existing vulnerabilities
- You will use indicators and hints given on the website: they will guide and help you!
- After the successful hunt for vulnerabilities, you will try to take advantage and exploit this vulnerability
- This specific vulnerability will grant you "the highest Science Fair points", which could make your team the winners of this competition...!